

**IN THE SPECIFICATION:**

**Page 30, lines 2-18, replace the Abstract of the Disclosure as follows:**

Master and slave Bluetooth-enabled devices communicate with other by sending messages using a carrier frequency that is constantly hopping from one frequency to another. In the prior art, each frequency in the sequence of frequencies, known as a hopping sequence, is determined as a known function  
5 of the master's Bluetooth address (BD\_ADDR) and a universal time parameter. A computer-strong eavesdropper who is listening to one or more frequency  
A, B, bands over a period of time and within range of a user's piconet could determine the BD\_ADDR of the user's device by comparing a detected hopping sequence with the hopping sequence associated with each possible BD\_ADDR. Once the  
10 BD\_ADDR of a user's device is determined, the user's location can thereafter be tracked as he moves from location to location using that device. To prevent this, the hopping sequence is determined as a known function of the master's BD\_ADDR, a universal time parameter and a seed, which is a random or pseudo-random number communicated between the master to the slave and  
15 which is changed each time a new session begins on one of the user's devices operating on the piconet. The eavesdropper is then impeded from associating a detected pattern of channel usage with a particular master's BD\_ADDR and its user.

**IN THE CLAIMS:**

**Replace Claims 1 - 40 with claims 41-80 as follows:**

**New Claim 41:**